IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF VIRGINIA
ROANOKE DIVISION

UNITED STATES OF AMERICA	)	
	)	Case No. 7:17cr00075
v.	)	
	)	By: Michael F. Urbanski
AKEEM ALEXIS BREWER, ET AL.	)	Chief United States District Judge

MEMORANDUM OPINION

Defendant Akeem Alexis Brewer ("Brewer") moves to modify or quash a search warrant for two Apple iPhones seized during his arrest for alleged distribution of heroin and conspiracy to distribute heroin in violation of 21 U.S.C. §§ 841 and 846. See Mot. to Quash or Modify Search Warrant, ECF No. 31. The search warrant authorized searching the phones for records relating to violations of 21 U.S.C. §§ 841 and 846, evidence of attribution showing who used or owned the devices at the time of the violations, stored photographs and videos depicting evidence of the violations, and records evidencing use of Internet Protocol addresses and internet activity. See Appl. and Aff. for Search Warrant, 7:17-mj-00129, ECF No. 1; Search and Seizure Warrant, 7:17-mj-00129, ECF No. 2.

During the course of briefing, the parties stipulated to the facts relevant to the application for and execution of the search warrant.[1] The government sought a search warrant on November 15, 2017 to conduct a forensic examination of the two seized iPhones and to compel Brewer's fingerprints to unlock the phones with touch ID. The court granted

[1] Brewer's motion to modify or quash the search warrant included certain allegations about the execution of the search warrant. At the March 6, 2018 hearing, however, Brewer's counsel clarified that there was no assertion of any misconduct by prosecution or law enforcement as regards Brewer's cell phones.

the warrant application on the same day. During the execution of the warrant, the government gained access to the first iPhone ("Device 1") through fingerprint access; Brewer and counsel agreed to provide the pass code for Device 1 to accommodate the government's access when Device 1 timed out. The second iPhone ("Device 2") did not have fingerprint access. The government gained access to Device 2 by using Device 1's pass code. The government conceded that the warrant did not grant access to Device 2 because it was not touch ID enabled, and that it "does not intend to view, examine or otherwise use the contents of Device 2." Parties' Stipulated Statement of Fact Pertaining to Def.'s Mot. to Quash, ECF No. 116, at 4. Pending this court's review of the warrant, the government also agreed to not examine the contents of Device 1.[2]

The court held a hearing on March 6, 2018 regarding whether to modify or quash the warrant. Counsel for Brewer limited his objection to the search warrant being overbroad and not sufficiently particular, and did not contest the search warrant's grant of fingerprint access to the devices via Touch ID. For Paragraphs 1 and 3 of Attachment B to the warrant—regarding records relating to violations of 21 U.S.C. §§ 841 and 846 and stored photographs and videos depicting evidence of the violations—Brewer argued that the government had no way to review these items without opening all of the files, and thus such a review is too broad given the nature of electronic files stored on phones.[3] Brewer requested use of a search protocol and abandonment of the plain view doctrine, as outlined in Judge Kozinski's

---

[2] This understanding was memorialized by an order entered by the magistrate judge on November 17, 2017. See Order, 7:17-mj-00129, ECF No. 3, at 2.

[3] Counsel for Brewer stated at the hearing that Brewer had no specific objection to Paragraph 2 of Attachment B regarding evidence of user attribution.

concurrence to United States v. Comprehensive Drug Testing, Inc., 621 F.3d 1162, 1178–1180 (9th Cir. 2010). For Paragraph 4, regarding records of Internet Protocol addresses and internet activity, Brewer argued that the request was overbroad because it was not limited to the violations at issue. Brewer also sought destruction of Device 2's copied data and destruction or return of all non-relevant items from Device 1.

The government confirmed the sequestration of the evidence from both devices and its agreement to not review the downloaded contents of Device 2. As for Device 1, the government argued that the only way to review Device 1's contents is to open the files and subsequently not use items irrelevant to the warrant. The government noted that the only case law cited by Brewer in support of a search protocol is a non-binding Ninth Circuit concurrence, and that the widely adopted approach is to determine admissibility after the evidence has been searched. As for Paragraph 4 regarding internet activity, the government contends that the search is not overly broad because it is only looking for evidence of criminal activity, such as travel arrangements relating to the drug conspiracy and the possible purchase of assault style weapons believed to be a part of the criminal activity. Pursuant to Federal Rule of Criminal Procedure 41(c), which is cited on the first page of the warrant, the government only seeks evidence of a crime for all aspects of the warrant. The government also represented that it is willing to destroy the copy of Device 2's electronic data, but wanted to maintain physical custody of the iPhone in the event the government had the opportunity to lawfully search it later in the investigation.

Given Brewer's evolving argument from the time of the motion to the time of the hearing, the court notes that the following issues are currently before it: (1) whether

Paragraphs 1 and 3 of Attachment B are sufficiently particular, including whether there is a need to impose search protocols, and (2) whether Paragraph 4 is overly broad.

I.

As to the first issue, it is clear that Paragraphs 1 and 3 of the warrant, specifying the search for records relating to violations of 21 U.S.C. §§ 841 and 846 and stored photographs and videos depicting evidence of the violations, are sufficiently particular.[4] The Fourth Amendment requires that a search warrant describe the things to be seized with sufficient particularity to prevent a "general, exploratory rummaging." Coolidge v. New Hampshire, 403 U.S. 443, 467 (1971). "This requirement ensures that the search is confined in scope to particularly described evidence relating to a specific crime for which there is probable cause." United States v. Oloyede, 982 F.2d 133, 138 (4th Cir. 1992). There is probable cause for the search of evidence relating to violations of 21 U.S.C. §§ 841 and 846, as the application contends that Brewer used Device 1 in his alleged drug-distribution activities. The government set forth in its warrant application that the devices were linked to the alleged drug violations. The search warrant's review of records, stored photographs, and videos also are limited to the specific violations at issue. Brewer does not appear to contest the limited scope of Paragraphs 1 and 3, but requests search protocols to limit the government's review of Device 1 so that the government cannot review records, photographs, and videos that do not reflect violations of 21 U.S.C. §§ 841 and 846 and further requests that a third-party conduct the review.

[4] To the extent Brewer has an objection to Paragraph 2, regarding evidence of attribution showing who used or owned the devices at the time of the violations, the court finds that the paragraph is sufficiently particular for the same reasons.

But this is not a case like Comprehensive Drug Testing, where the Ninth Circuit debated whether search protocols and third-party data review should be employed. Comprehensive Drug Testing arose out of the steroid scandal that rocked Major League Baseball in the early part of this century. As part of a collective bargaining agreement, players agreed to suspicionless drug testing of all players in an effort to determine whether ongoing testing was necessary. Although federal authorities learned of ten players who had tested positive in the Comprehensive Drug Testing program, law enforcement obtained a search warrant for Comprehensive Drug Testing's facility in Long Beach, California. When the warrant was executed, the government seized and promptly reviewed the drug testing records for hundreds of Major League Baseball players.

Motions to quash were filed, and the dispute was ultimately resolved by an en banc decision of the Ninth Circuit Court of Appeals. In a concurring opinion, Judge Kozinski offered some "guidance about how to deal with searches of electronically stored data." Id. at 1178. Judge Kozinski recommended employing a process that separated data defined by the warrant from other data, such as seizing only information belonging to people named in the warrant (rather than unnamed parties) or using hashing tools to identify well-known illegal files (such as child pornography) without opening the files themselves. Id. at 1179. "To that end, the warrant application should normally include, or the issuing judicial officer should insert, a protocol for preventing agents involved in the investigation from examining or retaining any data other than that for which probable cause is shown. The procedure might involve, as in this case, a requirement that the segregation be done by specially trained computer personnel who are not involved in the investigation." Id.

Concurring in part and dissenting in part, Judge Callahan disagreed. Id. at 1183–92. Judge Callahan viewed the suggestions as overbroad and unsupported by legal authority, referencing United States v. Giberson, 527 F.3d 882, 887–88 (9th Cir. 2008), where the Ninth Circuit declined to impose heightened Fourth Amendment protections in computer search cases as a result of a computer's ability to store large amounts of potentially intermingled information, and stating that such heightened protections must be "based on a principle that is not technology-specific." Id. at 1183. Moreover, Judge Callahan cautioned against jettisoning the plain view doctrine in digital evidence cases and found no legal support for requiring use of specialized personnel or an independent third party.

This case presents none of the concerns raised in Comprehensive Drug Testing. Comprehensive Drug Testing involved the government's seizure and review of digital test data of hundreds of individuals not implicated in the government's steroid use investigation. Here, in contrast, the cell phone at issue was located on Brewer's person and was alleged by the government to have been used by him in furtherance of the drug conspiracy. In this case, the court does not believe that the warrant must specify search term protocols or require that the search be done by independent third parties. The risk of commingling of data of uninvolved third parties present in Comprehensive Drug Testing is simply lacking here.

As such, the court will **DENY** the motion to quash the warrant as regards Paragraphs 1 and 3 of Attachment B, finding those paragraphs to be sufficiently particular and in compliance with Federal Rule of Criminal Procedure 41.

II.

Brewer presents a more compelling argument regarding Paragraph 4's search of his Internet Protocol addresses and internet activity. Paragraph 4 does not limit the search to violations of 21 U.S.C. §§ 841 and 846, which is inconsistent with the first three paragraphs of Attachment B. While the government contends that the warrant application's reference to Federal Rule of Criminal Procedure 41(c) limits this search to evidence of these crimes, the limitations ascribed to the first three paragraphs suggests a risk of an overbroad search for Internet Protocol addresses and internet activity beyond the drug-conspiracy violations and even the related gun allegations presented at the hearing.

Courts in the Fourth Circuit have upheld search warrants that broadly allow search and seizure of "[a]ny and all records, documents, invoices and materials that concern any accounts with any internet service provider." United States v. Young, 260 F. Supp. 3d 530, 549 (E.D. Va. 2017) ("Given the defendant's use of burner phones and anonymous email accounts for communication, it was reasonable to infer that he might have taken additional steps to conceal evidence of his interactions with FTOs. Courts have routinely upheld warrants authorizing the seizure of these types of information."). While broad searches of internet activity have been allowed, the court errs on the side of caution in protecting Brewer's Fourth Amendment rights and modifies the warrant to impose the same violation-specific limitation on Paragraph 4 as already implemented in Paragraphs 1, 2, and 3. Modifying the warrant to limit the scope of Paragraph 4 will not impede the government in its investigation because Device 1's data has been sequestered (thus not requiring

suppression) and the government represented at trial that it was only interested in Paragraph 4 evidence relevant to the criminal activity alleged.

Regarding the destruction of data downloaded from Device 2, the government already has represented that it will destroy the copy of Device 2's electronic data. Otherwise, Federal Rule of Criminal Procedure 41(f)(1)(B) allows an officer to "retain a copy of the electronically stored information that was seized or copied."

Therefore, the court **GRANTS in part** and **DENIES in part** Brewer's Motion to Modify or Quash Search Warrant (ECF No. 31) and hereby **ORDERS**:

1. Paragraph 4 of Attachment B of the search warrant issued on November 15, 2017 (ECF No. 2, 7:17-mj-00129) shall be **MODIFIED** to the following: "Records evidencing the use of the Internet Protocol addresses and records of internet activity that relate to violations of 21 U.S.C. §§ 841 and 846 and involve Akeem Alexis BREWER, including: a) records of Internet Protocol addressed used; b) records of Internet activity, including firewall logs, caches, browser history and cookies, 'bookmarked' or 'favorite' web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses."
2. The government shall destroy the downloaded copy of Device 2's data forthwith, and certify the destruction to Brewer's counsel. The government may retain physical custody of Device 2 in its possession, without examination, pending the trial of this case or further order of the court.

It is **SO ORDERED**.

Entered: March 21, 2018

/s/ Michael F. Urbanski

Michael F. Urbanski
Chief United States District Judge